

**THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

A.D., R.G., T.B., E.W., M.H., S.B., C.C., K.F.,)
C.M., A.O., A.H., and C.A.,)
individually and on behalf of all others similarly) No. 24 C 1404
situated,)
) Judge Virginia M. Kendall
Plaintiffs,)
v.)
) ASPEN DENTAL MANAGEMENT, INC.,)
) *Defendant.*)

MEMORANDUM OPINION AND ORDER

Plaintiffs A.D., R.G., T.B., E.W., M.H., S.B., C.C., K.F., C.M., A.O., A.H., and C.A., filed suit on behalf of themselves and a putative class of similarly situated persons against Aspen Dental Management (“Aspen”). Plaintiffs allege that Aspen embedded tracking pixels and other technology on its website to collect and transmit personally identifiable and protected health information to third parties like Facebook, Google, and Bing. (*See generally*, Dkt. 7 “FAC”). Aspen moves to dismiss Plaintiffs’ Complaint under Federal Rule of Civil Procedure 12(b)(6). (Dkt. 20). For the reasons below, Aspen’s motion [20] is granted in part and denied in part.

BACKGROUND

Defendant Aspen is a dental service organization that provides business support services to dentists, ranging from practice consulting to total practice management. (FAC ¶¶ 4, 68). One of the services Aspen provides is maintenance of the website located at <https://www.aspendental.com/> (the “Website”). (*Id.* ¶ 6). Individuals visiting the Website (“Users”), can search for information about a specific dental condition, locate providers, and schedule appointments and procedures. (*Id.* ¶¶ 6–7).

Plaintiffs and putative class members are individuals who use Aspen’s online platform. (*Id.* ¶¶ 53–67). They allege that Aspen disclosed their personally identifiable information (“PII”) and protected health information (“PHI”) to third parties, like Meta Platforms, Inc. d/b/a Meta (“Facebook”) and Google LLC d/b/a Google (“Google”), via tracking pixels, first-party cookies, and conversion application programming interface (“CAPI”) tools. (*Id.* ¶¶ 7–8, 10–20). Aspen configured and installed these tracking tools to bolster its profits by way of targeted advertisements that are created based on the private health information that the plaintiffs inputted on its website. (*Id.* ¶ 24).

Aspen’s tracking devices operate as follows: when an individual accesses a certain page or submits a search query on Aspen’s website, the individual’s browser sends a request to Aspen’s server to load the particular webpage. (*Id.* ¶¶ 23 n. 15, 203). At the same time, the tracking pixels embedded on Aspen’s website duplicate the communication and send it to third-party servers, like Facebook, alongside a transcription of the communication’s content and the individual’s identity. (*Id.* ¶¶ 106–11, 199–200, 203–07). Aspen’s tracking pixels are configured to collect Users’ sensitive health information, such as their status as patients, medical appointments, healthcare providers, medical conditions, and treatments. (*Id.*). This sensitive health information is then disclosed to companies, like Facebook and Google, alongside Users’ IP addresses and “unique Facebook IDs” which, in turn, is used to build marketing and other data profiles to identify, target, and market specific products and services to these individuals. (*Id.* ¶¶ 14, 29–30).

Plaintiffs filed suit on behalf of themselves and seven putative classes—a nationwide class and statewide classes in Illinois, Florida, Massachusetts, Washington, California, and Pennsylvania—whose private information was disclosed to third parties through the tracking pixels and related tracking technologies employed on Aspen’s online platform. (*Id.* ¶¶ 384–91).

The Complaint raises a federal claim under the Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. § 2511(1), et seq. (Count I), as well as state law claims for negligence (Count II), invasion of privacy (Count III), unjust enrichment (Count IV), breach of implied contract (Count V), violations of the Illinois Consumer Fraud and Deceptive Business Practices Act (“ICFA”), 815 ILCS 505/1, et seq. (Count VI), violation of the Illinois Eavesdropping Statute, 720 ILCS 5/14, et seq. (Count VII), violation of the Florida Security Communications Act (“FSCA”), Fla. Stat. § 934.01, et seq. (Count VIII), violation of the Massachusetts Consumer Protection Act (“MCPA”), M.G.L. § 93A, et seq. (Count IX), violation of the Massachusetts Wiretap Act (“MWA”), M.G.L. C. 272 § 99 (Count X), violation of the Washington Consumer Protection Act (“WCPA”), Wash. Rev. Code Ann. § 19.86.020, et seq. (Count XI), violation of the California Invasion of Privacy Act (“CIPA”), Cal. Penal Code § 630, et seq. (Count XII), violation of the California Confidentiality of Medical Information Act (“CMIA”), Cal. Civ. Code § 56, et seq. (Count XIII), violation of the California Unfair Competition Law (“UCL”), Cal. Bus. & Prof. Code § 17200, et seq. (Count XIV), and violation of the Pennsylvania Wiretap Act (“WESCA”), 18 Pa. Cons. Stat. § 5701, et seq. (Count XV). (FAC). Aspen moves to dismiss Plaintiffs’ class action complaint for failure to state a claim under Rule 12(b)(6). (Dkt. 20).

LEGAL STANDARD

A Rule 12(b)(6) motion tests whether the plaintiff has provided “enough factual information to state a claim to relief that is plausible on its face” and has raised “a right to relief above the speculative level.” *Haywood v. Massage Envy Franchising, LLC*, 887 F.3d 329, 333 (7th Cir. 2018) (citing *Camasta v. Jos. A. Bank Clothiers, Inc.*, 761 F.3d 732, 736 (7th Cir. 2014)). In deciding a Rule 12(b)(6) motion, the Court accepts as true all well-pleaded factual allegations and draws all reasonable inferences in favor of the non-moving party. *Lax v. Mayorkas*, 20 F.4th

1178, 1181 (7th Cir. 2021). Dismissal is proper where “the allegations ..., however true, could not raise a claim of entitlement to relief.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 558 (2007).

DISCUSSION

Before addressing Aspen’s arguments in support of dismissal, the Court notes that Plaintiffs withdrew several of their claims in their response brief, including their claims for invasion of privacy (Count III), breach of implied contract (Count V), and violation of the Massachusetts Consumer Protection Act (Count IX). These claims are therefore withdrawn, and the Court will not address them further.

Aspen challenges Plaintiffs’ Complaint on the grounds that the allegations are insufficient to state claims upon which relief may be granted. The Court addresses each argument in turn.

I. Electronic Communications Privacy Act

In Count I, Plaintiffs allege violations of the ECPA. The ECPA provides a private right of action against any person who “intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any ... electronic communication.” 18 U.S.C. § 2511(1)(a). The same is true for anyone who intentionally discloses or uses the contents of an intercepted communication. 18 U.S.C. §§ 2511(1)(c) & (d). Under the so-called “one-party exception,” the ECPA is not violated if the person intercepting the communication “is a party to the communication or where one of the parties to the communication has given prior consent to such interception.” 18 U.S.C. § 2511(2)(d). The one-party exception does not apply, however, if the “communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.” *Id.*

First, Aspen argues that Plaintiffs’ ECPA claim fails under the statute’s one-party exception because Aspen was a party to the communications and the crime-tort exception does not

apply. Aspen relies on *Desnick*, the leading Seventh Circuit opinion on this issue, which stands for the proposition that the crime-tort exception applies when the defendant had criminal or tortious intent at the time it committed the alleged violation, but not when the defendant later misused the intercepted communication in furtherance of a separate crime. *Desnick v. Am. Broad. Companies, Inc.*, 44 F.3d 1345 (7th Cir. 1995). In *Desnick*, the defendant sent testers armed with undercover surveillance devices into a doctor's office to see whether the doctor would recommend unnecessary cataract surgery on the testers, which the doctor did. *Id.* at 1353. Later, the defendant aired a broadcast featuring footage from the testers' office visits and describing the doctor's unscrupulous conduct. The doctor sued, bringing claims of defamation and violation of the ECPA. In reaching its conclusion that the crime-tort exception did not apply, the court focused on fact that defendant did not send testers to the doctor's office with recording equipment for the purpose of defaming the doctor by charging tampering with medical equipment.

The case at bar is distinguishable. Accepting Plaintiffs' allegations as true, as the Court must at this stage, Aspen placed tracking technology on its website with the intent to collect and disclose users' personal health information for purposes of financial gain, in violation of 42 U.S.C. § 1320d-6 of the Health Insurance Portability and Accountability Act ("HIPAA")

Section 1320d-6 of HIPAA imposes federal criminal liability for one who knowingly discloses "individually identifiable health information" ("IIHI") to third parties. IIHI is any information that:

(A) is created or received by a health care provider ... and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and – (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individuals. 42 U.S.C. § 1320(d)(6).

Here, Plaintiffs allege that Aspen, via the tracking devices employed on its webpages, transmitted Plaintiffs' patient status, medical conditions, information about their medical appointments and treatments, specific medical providers, and other sensitive health information to third parties. (FAC ¶ 173). Plaintiffs' allegations regarding their individual experiences using Aspen's online platform—and the inferences drawn from those experiences—are sufficient to plausibly allege that Aspen disclosed information regarding their personal health conditions and treatments to third parties. Such information qualifies as IIHI for purposes of HIPAA. Further, Plaintiffs allege that Aspen's collection and disclosure of their personal health information was done knowingly and for purposes of financial gain—namely, to bolster profits via targeted marketing campaigns. (*Id.* ¶¶ 264, 271, 456). Aspen claims that its only purpose was to improve its marketing and boost its revenues, but this purpose cannot be detached from the reality that Aspen achieved this improved marketing and revenue boost by disclosing Plaintiffs' IIHI. Taken as a whole, Plaintiffs' allegations are sufficient to invoke HIPAA for purposes of the ECPA's crime-tort exception.

Aspen secondarily argues that the crime-tort exception does not apply because the underlying criminal or tortious acts must be distinct from the alleged wiretapping. But Aspen does not cite to any precedential authority supporting this position and the Court is not aware of any. Even if the crime-tort exception did require an act distinct from the alleged wiretapping, Plaintiffs plausibly allege that Aspen intended to violate the HIPAA when it transmitted Plaintiffs' information to third parties, which is distinct from the improper interception at issue in the ECPA claim. Accordingly, Aspen's motion to dismiss Count I is denied.

II. State Wiretap Act Violations

A. Illinois Eavesdropping Statute

In Count VII, Plaintiffs allege violations of the Illinois Eavesdropping Statute. This statute creates a civil cause of action against an eavesdropper who knowingly, intentionally, and surreptitiously “[u]ses an eavesdropping device” to transmit or record “all or any part of any private conversation to which he or she is a party unless he or she does so with the consent of all other parties to the private conversation.” 720 ILCS 5/14-2(a)(2); *see also* 720 ILCS 5/14-6 (civil remedies). The definition of “eavesdropping device” includes any device capable of being used to intercept or transcribe electronic communications. 720 ILCS 5/14-1(a). The statute also prohibits the use or disclosure of any information which the eavesdropper “knows or reasonably should know was obtained from a private conversation or private electronic communication ... unless he or she does so with the consent of all of the parties.” 720 ILCS 5/14-2(a)(5).

Aspen contends that Plaintiffs cannot state a claim under the Illinois Eavesdropping Statute because the statute only applies to a person who is not a party to the communication. (Dkt. 21 at 9). Aspen is correct that the statute proscribes use of an eavesdropping device by a non-party for the purpose of “overhearing, transmitting, or recording all or any part of any private conversation,” 720 ILCS 5/14-2(a), but that is only one way in which the statute may be violated. Here, Plaintiffs allege violations based on use of an eavesdropping device “for the purpose of transmitting or recording all or any part of any private conversation to which he or she is a party.” (FAC ¶ 520) (citing 720 ILCS 5/14-2(a)(2)). That Aspen is alleged to have been a party to the intercepted communications is, thus, not fatal to Plaintiffs’ claim.

Aspen also argues that Plaintiffs cannot state a claim because the statute only applies to oral communications. The statute clarifies that “private conversation” means “any oral

communication between 2 or more persons, whether in person or transmitted between the parties by wire or other means.” 720 ILCS 5/14-1(d). Plaintiffs insist that communications over the internet are within the scope of this definition. In the briefing on this issue, neither party points to a relevant construction of the Illinois Eavesdropping Statute by the Illinois Supreme Court or any Illinois Court of Appeals. The text of the statute, however, appears to support Aspen’s construction.

After defining “private conversation,” the statute separately defines “private electronic communication” to mean “any transfer of ... writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system.” 720 ILCS 5/14-1(e). The difference in these definitions suggests legislative intent to distinguish between the disclosure of conversations, like those occurring in-person or over the phone, and electronic communications, like the private user data and appointment scheduling information at issue here. (*See generally* FAC ¶¶ 113, 527–29).

For the purposes of this motion and based on the briefing before the Court, the Court concludes that 720 ILCS 5/14-1(d) does not apply to the electronic communications about which Plaintiffs complain. Accordingly, Count VII is dismissed.

B. Massachusetts Wiretap Act

In Count X, Plaintiffs allege that Aspen violated the MWA. Aspen asserts that Plaintiffs’ MWA claim fails because the MWA excludes activities undertaken in the ordinary course of business from the statutory definition of an unlawful “interception.” Mass. Gen. Laws Ann. ch. 272, § 99(B)(3). Plaintiffs argue that the exception does not apply here because, they claim, using tracking technology to send user information to third parties is not part of Aspen’s ordinary course of business. While Aspen is in the business of providing support to dental practices, even the

Complaint alleges that the Website routinely collected and transmitted Users' PHI to third parties for the purpose of generating revenue. (FAC ¶¶ 87, 107, 113). The most reasonable inference, then, is that the actions underlying Plaintiffs MWA claim were a part of Aspen's ordinary course of business. Indeed, the ability to target marketing towards viable consumers is an "unavoidable byproduct or consequence" of doing business in the modern age. *Dillon v. Massachusetts Bay Transp. Auth.*, 49 Mass. App. Ct. 309, 319 (2000) (citing *Amati v. Woodstock*, 176 F.3d 952, 956 (7th Cir.), *cert. denied*, 528 U.S. 985 (1999)). Targeted marketing, facilitated by tracking one's online activity, is so pervasive that it is "apt to be known" and is properly considered within the bounds of Aspen's ordinary course of business. *Amati*, 176 F.3d at 955. Thus, Aspen's motion to dismiss Count X is granted.

C. Florida Security of Communications Act, California Information Privacy Act, and Pennsylvania Wiretap Act

In Counts VIII, XII, and XV, Plaintiffs claim that Aspen violated various state consumer protection acts, including the FSCA, WESCA and CIPA, when it used the Pixel and other tracking technology to intercept their communications with Aspen's website and transmit that information to third parties. Aspen argues Plaintiffs cannot state a claim under any of these statutes. The Court considers each argument in turn.

1. Contents of Communication

According to Aspen, Plaintiffs have not sufficiently alleged that any "contents" of a communication were intercepted. This argument applies to the FSCA, WESCA, and CIPA claim. The FSCA, WESCA, and CIPA, like many states' wiretapping laws, were modeled after the ECPA. As a result, Florida, Pennsylvania, and California courts look to federal courts as to the meaning of analogous provisions, including what constitutes "contents" of a communication. *See, e.g., Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 125–126 (3d Cir. 2022) (WESCA "operates

in conjunction with and as a supplement to the Federal Wiretap Act, 18 U.S.C. § 2150 et seq.”); *Minotty v. Baudo*, 42 So.3d 824, 831 (Fla. 4th Dist. Ct. App. 2010) (noting that “Florida follows federal courts as to the meaning of provisions after which Chapter 934 was modeled”); *Gutierrez v. Converse Inc.*, 2023 WL 8939221, at *3 (C.D. Cal. Oct. 27, 2023) (the “CIPA fails to define ‘contents,’ [so] federal courts look to the analogous Federal Wiretap Act for guidance”). “Contents” of a communication include “any information concerning the substance, purport, or meaning of that communication.” 18 U.S.C. § 2510(8) (defining “contents”); Fla. Stat. Ann. § 934.02 (same); 18 Pa. Cons. Stat. Ann. § 5702 (same).

Aspen argues that Plaintiffs’ allegations are insufficient to show that the “contents” of their communications were disclosed because data like URLs from Plaintiffs’ browsing history—which included Plaintiffs’ search terms about medical conditions and types of treatments—are not properly considered the type of content covered under the state wiretapping statutes at hand. Courts interpreting contents under the ECPA distinguish between “a record or other information pertaining to a ... customer” (known as “record information”) and the contents—i.e., “substance, purport, or meaning”—of the communication itself. *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014) (quotations omitted) (“[T]he term ‘contents’ refers to the intended message conveyed by the communication, and does not include record information.”).

With respect to metadata like URLs, courts have differentiated between those that provide “basic identification and address information,” and those that disclose a “search term or similar communication made by the user.” *See Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d 1064, 1076 (N.D. Cal. 2023) (citing *In re Zynga Priv. Litig.*, 750 F.3d at 1108–09). Such courts have reasoned that while the former constitutes record information, the latter qualifies as “content” for purposes of the ECPA. *See id.*; *see also In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806

F.3d 125, 137 (3d Cir. 2015) (“URLs may be dialing, routing, addressing, or signaling information, but only when they are performing such a function.” If instead a URL is “part of the substantive information conveyed to the recipient, then by definition it is ‘content.’”). In this case, the URLs at issue include terms entered into search fields and fillable forms. (FAC ¶ 140). This is sufficient to plausibly allege that covered “content” was intercepted. *See, e.g., In re Grp. Health Plan Litig.*, 2023 WL 8850243, at *7; *Meta Platforms, Inc.*, 690 F. Supp. 3d at 1076–77.

2. Device

Next, Aspen argues that Plaintiffs fail to plausibly allege that a “device” was used to intercept the communications. This argument applies to the FSCA and WESCA claims. The FSCA and WESCA, like the ECPA, defines “electronic, mechanical, or other device” as “any device or apparatus which can be used to intercept a wire, oral, or electronic communication” with a few exceptions for tangible items such as telephones, hearing aids. *See* 18 U.S.C.A. § 2510(5); Fla. Stat. Ann. § 934.02(4); 18 Pa. Cons. Stat. Ann. § 5702. The MWA defines “intercepting device” as “any device or apparatus which is capable of transmitting, receiving, amplifying, or recording a wire or oral communication.” Mass. Gen. Laws Ann. ch. 272, § 99(B)(3).

Whether software is properly considered a “device” within the meaning of these statutes is unsettled. *See e.g., Jacome v. Spirit Airlines, Inc.*, No. 2021 WL 3087860, at *4 (Fla. Cir. Ct. June 17, 2021) (finding it persuasive that other courts have held that “software” does not constitute a “device”) (first citing *Potter v. Havlicek*, 2008 WL 2556723, at *8 (S.D. Ohio June 23, 2008); then citing *Ideal Aerosmith, Inc. v. Acutronic USA, Inc.*, 2007 WL 4394447, at *4 (E.D. Pa. Dec. 13, 2007)). *But see Makkinje v. Extra Space Storage, Inc.*, 2022 WL 80437, at *2 (M.D. Fla. Jan. 7, 2022) (finding persuasive that the “Eleventh Circuit has determined that software can constitute a

‘device’ in the wiretapping context”) (citing *United States v. Barrington*, 648 F.3d 1178, 1203 (11th Cir. 2011)).

Here, Plaintiffs allegations include a plausible explanation of how the tracking technology employed by Aspen captured information communicated by website users and transmitted that information to third parties. (FAC ¶¶ 11, 17, 92-94, 116, 132). Absent contrary authority, Plaintiffs allegations are sufficient to support their assertion the tracking technology Aspen employed is properly considered a “device.”

3. Electronic Communications

Aspen also argues that Plaintiffs fail to allege that any “electronic communications” were intercepted. This argument applies to the FSCA and WESCA claims. Like the ECPA, the FSCA and WESCA define “electronic communication” as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.” 18 U.S.C. § 2510(12) (defining “electronic communication”); Fla. Stat. Ann. § 934.02(12) (same); 18 Pa. Cons. Stat. Ann. § 5702 (same). As with the term “device,” it is unsettled whether information entered into a search field or online form constitutes an “electronic communication.” See *Jacome*, 2021 WL 3087860, at *3–5 (session replay software did not capture “electronic communications”); *Goldstein v. Costco Wholesale Corp.* (“*Costco*”), 559 F. Supp. 3d 1318, 1322 (S.D. Fla. 2021) (ruling that the FSCA does not apply to claims regarding session replay software). But see *Katz-Lacabe v. Oracle Am., Inc.*, 2023 WL 6466195, at *5 (N.D. Cal. Oct. 3, 2023), *aff’d*, 2023 WL 7166815 (N.D. Cal. Oct. 30, 2023) (transmissions containing “data entered by the user into forms” and certain URLs “constitute electronic communications under the FSCA”). Once again, neither side cites to binding precedent on this issue and, in the absence of

contrary authority, Plaintiffs' allegations plausibly state that the tracking technology transmitted their data, writing, and signals through a covered system that affects interstate commerce.

4. Location of Interception

According to Aspen, Plaintiffs do not sufficiently allege that the interception occurred within Pennsylvania as required to state a claim under the WESCA. Here, Plaintiffs allege that they used Aspen's website in Pennsylvania and that the tracking technology at issue works by planting a bug on users' browsers. The only reasonable inference to draw from these facts is that the tracking technology picked up Plaintiffs' communications from their web browsers, located in Pennsylvania. Based on these allegations, Plaintiffs plausibly allege that Aspen's interception occurred on Plaintiffs' browser, located in Pennsylvania. Ultimately, Plaintiffs bear the burden of proving that the interception actually occurred in Pennsylvania but, at this point, the "factual content" of the pleadings are sufficient to allow the Court to "draw the reasonable inference that [Aspen] is liable for the alleged misconduct." *Boucher v. Fin. Sys. of Green Bay, Inc.*, 880 F.3d 362, 366 (7th Cir. 2018) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)).

5. In Transit

Finally, Aspen argues that Plaintiff C.M. fail to state a claim under the CIPA because they do not allege that C.M.'s communications were intercepted while "in transit," as required by the CIPA. Aspen argues that no communication could be intercepted "in transit" because two separate communications occur: one between Aspen's website and Users' browser, and one between the User's browser and a third party, like Facebook. That Aspen disagrees with Plaintiff's factual allegation is insufficient to justify dismissing Plaintiff's CIPA claim. C.M. contends that Aspen both "use[d] source code to commandeer the User's computing device, causing the device to contemporaneously and invisibly re-direct the Users' communications to third parties" and

“employed ... tracking technologies, to intercept, duplicate, and re-direct Plaintiffs’ ... Private Information” to third parties. (FAC ¶¶ 105–07, 114–15). Though Plaintiff will bear the burden of proving each element of their claim, the allegations in the Complaint are sufficient to plausibly allege that Plaintiff’s communications were intercepted in transit.

Accordingly, Aspen’s motion to dismiss is denied with respect to Counts VIII, XII, and XV.

III. State Consumer Protection Claims

A. ICFA

In Count VI, Plaintiffs A.D, R.G., C.C. and K.F. allege that Aspen engaged in deceptive acts and practices in violation of the ICFA. “In order to state a claim under the ICFA, a plaintiff must show: ‘(1) a deceptive or unfair act or promise by the defendant; (2) the defendant’s intent that the plaintiff rely on the deceptive or unfair practice; and (3) that the unfair or deceptive practice occurred during a course of conduct involving trade or commerce.’” *Camasta v. Jos. A. Bank Clothiers, Inc.*, 761 F.3d 732, 739 (7th Cir. 2014) (quoting *Wigod v. Wells Fargo Bank, N.A.*, 673 F.3d 547, 574 (7th Cir. 2012)). The plaintiff must also “plausibly plead that the deceptive or unfair act caused her to suffer actual damages, meaning pecuniary loss.” *Benson v. Fannie May Confections Brands, Inc.*, 944 F.3d 639, 647 (7th Cir. 2019) (citing *Kim v. Carter’s Inc.*, 598 F.3d 362, 365 (7th Cir. 2010)).

Aspen argues that Plaintiffs’ ICFA claim cannot proceed because Plaintiffs (1) fail to allege deception; (2) they have not pleaded actual, pecuniary loss; (3) and they cannot establish an ICFA claim based on the Illinois Personal Information Protection Act (“PIPA”). Because Plaintiffs failed to allege the specific economic damages necessary to bring their claim under the ICFA, the Court begins and ends its analysis there.

The ICFA provides remedies for “purely economic injuries.” *Flores v. Aon Corp.*, 2023 IL App (1st) 230140, ¶ 41 (Ill. App. Ct. Sep. 29, 2023) (citing *Morris v. Harvey Cycle & Camper, Inc.*, 392 Ill.App.3d 399 (Ill. App. Ct. 2009)). “Actual damages must be calculable and ‘measured by the [plaintiffs’] loss.’ ” *Morris*, 331 Ill.Dec. 819, 911 N.E.2d at 1053 (quoting *Chicago v. Mich. Beach Hous. Coop.*, 297 Ill.App.3d 317, 231 Ill.Dec. 508, 696 N.E.2d 804, 811 (Ill. App. Ct. 1998)). “The failure to allege specific economic damages precludes a claim brought under the [ICFA].” *Flores*, 2023 IL App (1st) 230140, ¶ 41.

Plaintiffs allege that they suffered actual monetary loss in the form of “overpaying” for Aspen’s health services. (FAC ¶ 516). They also say that they used Aspen’s online platform based on it’s representation that their personal health information would be protected and not disclosed to unauthorized third parties. (FAC ¶¶ 9–10, 506). Plaintiffs, however, do not allege that but for Aspen’s representations they would not have used its services or would have paid less for those services. Even if they had, this type of “benefit of the bargain” theory of damages, however, has been repeatedly rejected for non-products liability claims such as this. *See Lewert v. P.F. Chang’s China Bistro, Inc.*, 819 F.3d 963, 968 (7th Cir. 2016) (citing *Remijas*, 794 F.3d at 695) (explaining that benefit of the bargain theories “have been adopted by courts only where the product itself was defective or dangerous and consumers claim they would not have bought it (or paid a premium for it) had they known of the defect”); *cf. In re Aqua Dots Prods. Liab. Litig.*, 654 F.3d 748, 751 (7th Cir. 2011) (acknowledging financial injury when plaintiffs “paid more for the toys than they would have, had they known of the risks the beads posed to children”). Plaintiffs do not cite any authority that would otherwise support a benefit of the bargain theory in the context of data privacy. *Cf. Kurowski v. Rush System for Health (“Kurowski II”)*, 683 F. Supp. 3d 836, 846 (N.D. Ill. 2023)

(declining to expand the benefit of the bargain theory to plaintiffs' ICFA claim based on the defendant's failure to protect private health information).

Accordingly, Plaintiffs' benefit of the bargain theory does not plausibly allege a monetary loss for purposes of the ICFA. Plaintiffs should note that they also cannot rely on allegations that Aspen's conduct caused a diminution in value of their personal data to allege an actionable harm for purposes of the ICFA. *See, e.g., Flores*, 2023 IL App (1st) 230140, ¶ 42 (declining to hold that "diminution in the value of personal information is a specific economic injury under the [ICFA]"). Aspen's motion to dismiss Count VI is therefore granted.

B. Washington Consumer Protection Act ("WCPA") and California Unfair Competition Law ("CUC")

In Count XI and Count XIV, Plaintiffs allege that Aspen engaged in deceptive acts or practices in violation of the WCPA and CUC. To state a claim under the WCPA, a plaintiff must allege that they "sustained damage to business or property." *Keodalah v. Allstate Ins. Co.*, 194 Wn.2d 339, 349–50 (2019). To state a claim under the CUC, a plaintiff must allege that they "lost money or property." *Kwikset Corp. v. Superior Ct.*, 51 Cal. 4th 310, 317 (2011); *Rubio v. Capital One Bank*, 613 F.3d 1195, 1203 (9th Cir. 2010). As set forth *supra* § III.A., Plaintiffs fail to satisfy this requirement. Thus, Counts XI and XIV are dismissed. *See Gragg v. Orange Cab Co., Inc.*, 942 F. Supp. 2d 1111, 1118–19 (W.D. Wash. 2013) (dismissing WCPA claim where alleged injury was privacy violation); *Panag v. Farmers Ins. Co. of Wash.*, 166 Wn.2d 27, 57 (2009) ("[p]ersonal injuries, as opposed to injuries to 'business or property,' are not compensable and do not satisfy the injury requirement").

C. California Confidentiality of Medical Information Act ("CMIA")

In Count XIII, Plaintiff C.M., on behalf of the California subclass, alleges that Aspen disclosed Plaintiff's medical information to unauthorized persons without first obtaining consent,

in violation of the CMIA. Cal. Civ. Code § 56.10(a). Aspen argues that Plaintiff C.M. fails to state a claim under the CMIA because C.M. does not allege that medical information was transmitted, and C.M. does not allege that any individual viewed or accessed their information.

The CMIA defines “medical information” as “any individually identifiable information” possessed by or derived from a healthcare provider or contractor “regarding a patient’s medical history, mental health application information, reproductive or sexual health application information, mental or physical condition, or treatment.” Cal. Civ. Code § 56.05(j). “Individually identifiable information” includes all information containing “any element of personal identifying information sufficient to allow identification of the individual, such as the patient’s name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the identity of the individual.” *Id.*

Here, C.M. claims that the information sent to third parties “included which Users were searching for a specific treatment, looking at pricing for a specific treatment or scheduling an appointment at a specific location for a specific treatment sought.” (FAC ¶ 145). That third parties were apprised of which medical care a specific user was looking for is not enough to sustain a claim under the CMIA. Plaintiff fails to allege that the disclosed information necessarily reveals information about their “physical condition or treatment” as required by the CMIA. A person could very well search treatments, medical conditions, and potential providers for a partner, parent, or child. A person could also search for treatment that they ultimately do not need or are not eligible to receive. At this stage, Plaintiff’s allegations do not plausibly allege that their medical information was transmitted. Thus, Count XIII is dismissed.

IV. Common Law Claims

A. Negligence

In Count II, Plaintiffs assert a claim for common law negligence. To state a claim for negligence under Illinois law, “a plaintiff must plead that the defendant owed a duty of care to the plaintiff, that the defendant breached that duty, and that the breach was the proximate cause of the plaintiff’s injuries.” *Cowper v. Nyberg*, 390 Ill.Dec. 115, 28 N.E.3d 768, 772 (Ill. 2015) (citing *Mt. Zion State Bank & Tr. v. Consol. Commc’ns, Inc.*, 169 Ill.2d 110, 214 Ill.Dec. 156, 660 N.E.2d 863, 867–68 (Ill. 1995)).

Aspen argues that Plaintiffs have not alleged that it owed Plaintiffs a duty of care beyond that of physician-patient confidentiality, and such a duty is insufficient to support a negligence claim because Illinois has not recognized an independent tort claim for breach of physician-patient confidentiality. (Dkt. 21 at 35). But Defendants fail to acknowledge Plaintiffs’ allegation that Aspen owed Plaintiffs a duty to “exercise reasonable care to secure, safeguard and protect their highly sensitive Private Information” and that Aspen assumed a duty to protect Plaintiffs Private Information by making representations that it would not disclose Plaintiffs’ Private Information without their consent. (FAC ¶¶ 9–10, 440). Plaintiffs’ position is supported by PIPA which requires data collectors, *i.e.*, entities that handle, collect, disseminate, or otherwise deal with nonpublic personal information, to protect this information from “unauthorized access, acquisition, destruction, use, modification, or disclosure.” 815 ILCS 530/45(a); *see also* 815 ILCS 530/5. The Complaint alleges that Aspen collected Plaintiffs’ nonpublic personal information and disseminated that information to unauthorized third parties. Thus, the complaint plausibly alleges a duty to prevent the disclosure of their private health information.

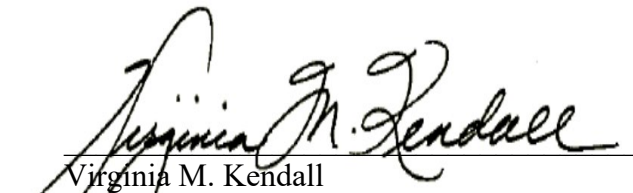
B. Unjust Enrichment

In Count IV, Plaintiffs plead a claim for unjust enrichment. Unjust enrichment, however, “is not a separate cause of action under Illinois law.” *Horist v. Sudler & Co.*, 941 F.3d 274, 281 (7th Cir. 2019); *see also Benson*, 944 F.3d at 648 (citing *All. Acceptance Co. v. Yale Ins. Agency, Inc.*, 271 Ill.App.3d 483, 208 Ill.Dec. 49, 648 N.E.2d 971, 977 (Ill. App. Ct. 1975), relying on *Charles Hester Enters., Inc. v. Ill. Founders Ins. Co.*, 137 Ill.App.3d 84, 91 Ill.Dec. 790, 484 N.E.2d 349, 354 (Ill. App. Ct. 1985), *aff’d*, 114 Ill.2d 278 (1986)). “[I]f an unjust enrichment claim rests on the same improper conduct alleged in another claim, then the unjust enrichment claim will be tied to this related claim—and, of course, unjust enrichment will stand or fall with the related claim.” *Cleary v. Philip Morris Inc.*, 656 F.3d 511, 517 (7th Cir. 2011); *see also Flores*, 2023 IL App (1st) 230140, ¶ 37.

Like their ICFA claim, Plaintiffs’ unjust enrichment claim alleges that Aspen collected and used Plaintiffs’ personal health data for its own financial gain and retained those benefits at Plaintiffs’ expense. (FAC ¶¶ 468–69.) Because that is the same improper conduct alleged in their ICFA claim, the Plaintiffs’ unjust enrichment claim cannot stand. *See, e.g., Ramirez v. LexisNexis Risk Sols.*, — F. Supp. 3d —, No. 22 C 5384, 2024 WL 1521448, at *8 (N.D. Ill. Apr. 8, 2024). Aspen’s motion to dismiss Count IV is therefore granted.

CONCLUSION

For the reasons set forth above, Aspen’s motion [20] is granted in part and denied in part.


Virginia M. Kendall
United States District Judge

Date: September 9, 2024